REMARKS

The Examiner has rejected 1, 3, 5-7, 9-10, 12, 14-16, 18-20, 22-24, 26, 28-30, 32-33, 36-37, 39, 42-43, 45-46, 50-51, 55-57, 59, 61, 63, 65-66, 69, 72, and 74-77 under 35 U.S.C. 103(a) as being unpatentable over Steinberg (U.S. Patent No. 6,587,949) in view of Matsushita (European Patent Application No. 00309498.4) in further view of Friedman (U.S. Patent No. 5,499,294). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to the independent claims.

With respect to all of the independent claims, the Examiner has relied on Col. 5, lines 52-57 in Steinberg to make a prior art showing of applicant's claimed "... validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames" (see this or similar, but not identical language in each of the independent claims).

> "A user's only clue concerning the unique nature of this device is that encrypted data loaded into a computer from the device will not be intelligible until decrypted, a process requiring special software in the computer, including a password and/or key." (Steinberg, Col. 5, lines 52-57 - emphasis added)

Applicant respectfully asserts that such excerpt merely teaches that the encrypted data on the device requires the user to decrypt it using "... special software on the computer, including a password and/or key." Cleary, such teaching does not even suggest any sort of "validating the decryption cryptographic key against user-provided credentials," as claimed by applicant (emphasis added). Instead, the excerpt only discloses that a password and/or key is used in combination with special software on the computer.

In the latest Office Action dated 02/08/2006, the Examiner has further argued that, "in order for decryption to ensue, a user may have to validly present both a

decryption key against user-provided credentials" before decrypting the encrypted frames. Simply presenting both a key and a password for decryption purposes, as allegedly set forth in Steinberg, simply do not rise to the level of specificity of applicant's claimed validation of one against the other. Again, only applicant teaches and claims "validating the decryption cryptographic key against user-provided credentials" (emphasis added), for validating the key itself, for example.

Still with respect to each of the independent claims, the Examiner has relied on the excerpts below in Steinberg to make a prior art showing of applicant's claimed technique "wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption cryptographic keys" (see this or similar, but not identical language in each of the independent claims).

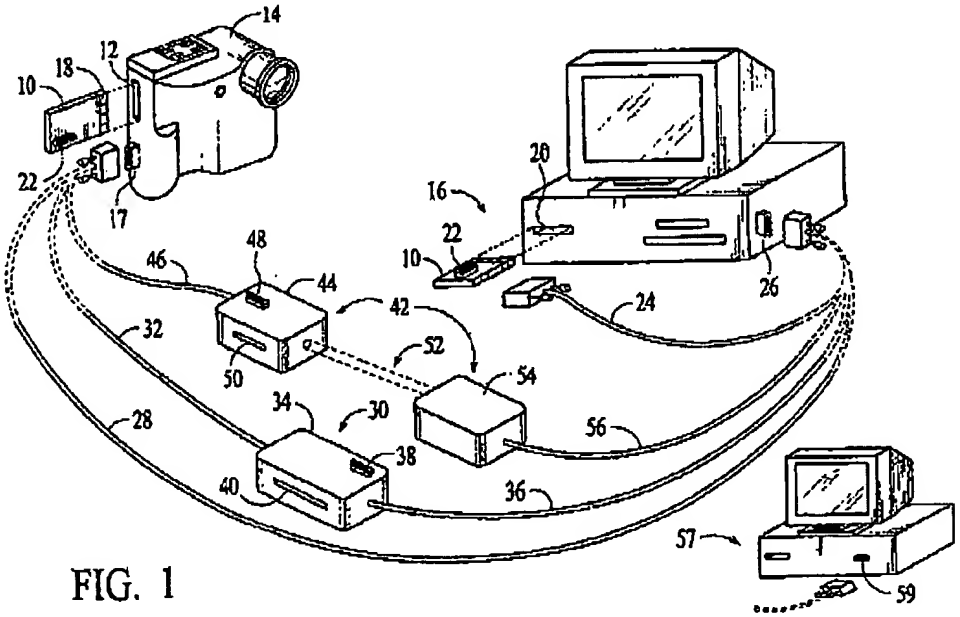

FIG. 1

(Steinberg, Figure 1)

"Alternatively, the device 10 can receive data through an input port 22 connected for example with a cable assembly 24 to a compatible port 26 of PC 16." (Steinberg, Col. 3, lines 59-61 - emphasis added)

"The device 10 is configured so that the PC 16 recognizes the device 10 as a regular storage device with readable files on the file system level without the need for presenting a password. The secure data is then transferred from the device 10 to the computer 16. In order for a user to view encrypted data, the computer 16 must be programmed to decrypt the data, generally in response to entry of a password." (Steinberg, Col. 4, lines 4-11 - emphasis added)

Applicant respectfully asserts that such excerpts teach two different connection methodologies. The first excerpt teaches that the direct cable connection to the PC is used so the device 10 may receive data from the PC 16 via device 10 port 22. The second excerpt relied upon by the Examiner merely teaches that the PC 16 utilizes the device 10 as a regular storage device where data is then transferred from device 10 to the computer 16. Neither of these references cited above, however, even mention applicant's claimed technique "wherein the removable storage medium includes memory that is coupled to a standardized connector which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption cryptographic keys" (emphasis added), as claimed.

In the latest Office Action dated 02/08/2006, the Examiner has responded to applicant's arguments by relying on item 10 and 16 of Figure 1 in Steinberg to meet applicant's specific claim language. After careful review of the entire Steinberg reference, applicant notes that Col. 4, lines 12-21 further clarifies Steinberg's disclosure on the use of the storage medium.

"Referring again to FIG. 1, according to the prior art, a digital camera 14 is connected to a computer 16 by way of a direct cable connection indicated by line 28 making a direct cable connection from the camera connector 29 to the PC connector 26. In this manner, unsecured camera data is directly transferred to a PC 16. An unauthorized user could then easily modify the data with the

> PC 16. The method and apparatus of the present invention solves this problem by first transferring the camera data to the secure storage device 10, which automatically secures the data." (Steinberg, Col. 4, lines 12-21 - emphasis added)

The Steinberg excerpt referenced above teaches that the device 10 (PCMCIA) may be directly connected to the computer 16 (PC) by way of a direct cable connection. When using this direct cable connection, the "unsecured camera data is directly transferred to a PC 16" (emphasis added). This reference thus fails to meet applicant's claimed technique "which enables utilization of at least one of a plurality of encryption cryptographic keys and a plurality of decryption cryptographic keys" (emphasis added). Thus, there are simply no teachings in Steinberg that the direct cable connection from the device 10 to PC 16 specifically enables the utilization of encryption keys and decryption keys.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of Claims 9, 18, 50, and 55 into each of the independent claims.

"wherein a set of cryptographic instructions is stored on the removable storage medium for employing at least one of the encryption cryptographic key and the decryption cryptographic key" (see this or similar, but not necessarily identical language in each of the independent claims).

Further, it appears that the Examiner has supported his primary arguments by relying on a computing system to meet applicant's claimed "removable storage medium," as claimed. To emphasize the clear distinction between an entire computing system (such as that in Steinberg), and applicant's claimed "removable storage medium," applicant has even further amended each of the independent claims, as follows:

"wherein the removable storage medium comprises only the memory and is separate from a player which is capable of playing the video content on the transportable storage medium" (see this or similar, but not necessarily identical language in each of the independent claims).

A notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The

Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P374/01.101.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120

408-505-5100